Sec-IoT: A framework for secured decentralised IoT using blockchain-based technology

Muhidul Islam Khan[1] and Isah A. Lawal[2]

[1] Tallinn University of Technology, Tallinn, Estonia
[2] Noroff University College, Kristiansand, Norway
mdkhan@ttu.ee
Isah.Lawal@noroff.no

Abstract. Blockchain technology has been used recently as a secure method for authenticating digital information in many applications. Inspired by the success of the technology, we envision the potential of the blockchain for secured communication in a decentralised Internet of Things (IoT). In this paper, we envisage a framework for a secured IoT and describe the infrastructure and mechanism of the entire system. Also, we provide solutions to overcome some of the limitations of blockchain technology including miner selection and reaching consensus, for a decentralised IoT by incorporating a learning to rank method for node selection. We also contemplate using hybrid consensus algorithm in the blockchain to detect faulty node and to improve the node convergence.

Keywords: Decentralised IoT; Blockchain technology; Learning to rank

1 Introduction

Internet-of-Things (IoT) is a network of devices connected via the internet. Several applications have been deployed over IoT space leveraging the ubiquitousness of sensors, actuators, radio-frequency identification (RFID) and communication protocols [14]. The classical centralised communication method commonly used for IoT is problematic for secured IoT because it is prone to failure [9]. A decentralised communication method typical of peer to peer networks can, however, improve the reliability of IoT. But security is a serious concern for decentralised communication. This is because IoT devices are used in many cases to collect and transmit sensitive data, keeping these data secure and accessible to only authorized entities is vital for many IoT applications. Recently, blockchain technology appeared as a trusted peer to peer communication method in many applications [3, 5, 6]. The technology is capable of handling an enormous amount of data in a secured manner using a distributed ledger technique. Data communication in the blockchain is done by creating blocks, where each block represents a single data transaction. Each transaction is verified using a mechanism known as mining and the devices involved in the process are called the miners [7]. Moreover, blockchain ensures security via cryptography, whereby blocks are encrypted using hashing techniques [8]. In this paper, we adopt the blockchain technology for secured

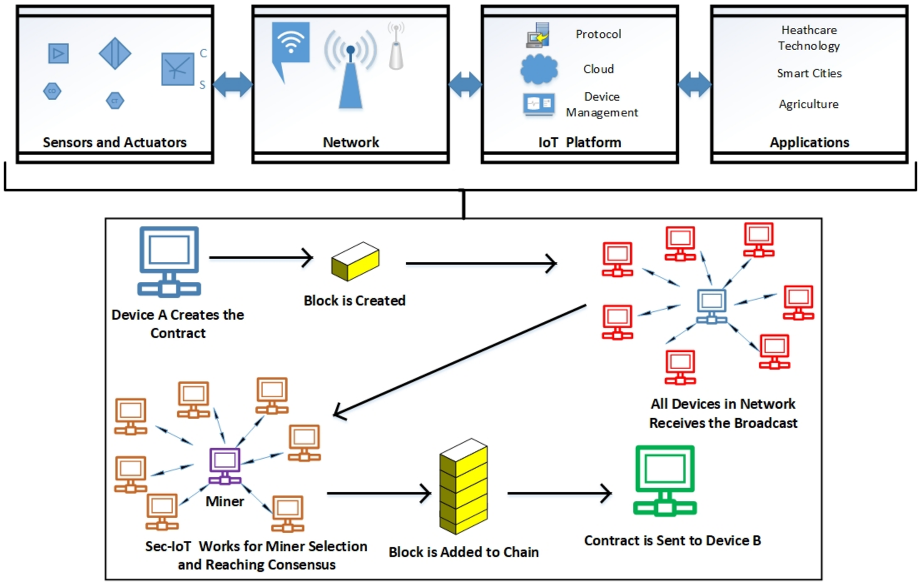

Fig. 1. Blockchain-based secured decentralised communication in IoT. **Top:** A generic IoT setup consisting of the following components; sensors/actuators, network, platform, and applications. **Bottom:** The blockchain mechanism applicable to any of the IoT components.

communication in a decentralized IoT. We propose a generalized security framework for IoT with consideration to important functionalities and requirements of the IoT such as an adaptive way to select the miners, encryption standard and consensus algorithm. Specifically, we incorporate a learning-to-rank method for miner selection in the blockchain for the decentralised IoT. We also propose a hybrid consensus algorithm to hasten convergence and to detect compromised miners.

2 The Sec-IoT framework

Figure 1 shows the proposed framework. We consider a generic IoT setup with several IoT devices (i.e. sensors, actuators) for any particular application (i.e., healthcare, smart cities, agriculture, etc.) which are connected through a communication technology (i.e., Wifi, Bluetooth, Wimax, LTE-advanced, etc.) using IoT based protocol, cloud infrastructure, and device management. The devices (also referred to as nodes) are distributed in terms of computing and data processing. The nodes are grouped into different networks with each network comprising of some special nodes, called the miners. These nodes have the most computing power, faster hash rate generation, and lower block propagation delay. Communication between two different miners is achieved through the consortium blockchain strategy shown in Figure 2. A consortium blockchain is a

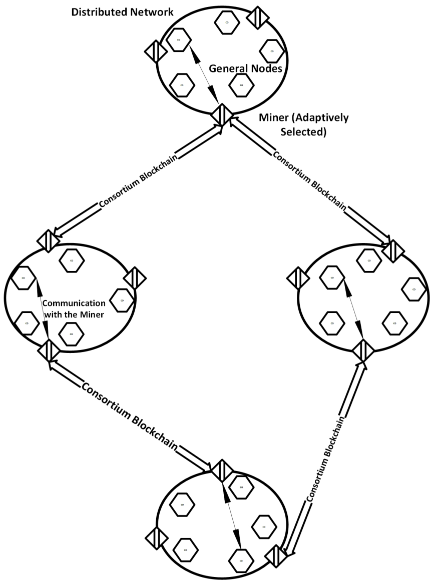

Fig. 2. Consortium blockchain mechanism. The circles represents a four networks consisting of general nodes (diamond shape) and miners (rectangular shape). The arrows represent communication with the general node and the miners, respectively

concept that incorporates the efficiency and privacy of private blockchain while leveraging the decentralized governance of public blockchain [4]. To transfer data from one node to another, the sending node must initiate the communication by creating a contract. The contract then undergoes a two-phase verification process. Firstly a miner is selected from the sending node network. This miner is responsible for generating an eligible signature for the contract and forwarding the signed contract to other miners in the network. Secondly, a consensus process whereby the miners examine the authenticity of the signed contract is executed. If the signature is genuine, a block is created for the signed contract. Figure 3 illustrates the process of reaching consensus among the miners in a network. The newly created block is added to a chain of other blocks and delivered to the receiving node. The miners then record the new blockchain information in a shared record system that is continuously updated, after each block verification process [16]. Because the record system is distributed across all the miners, ensures its authenticity over time. The processing power of miners is very important for verification of contracts in blockchain. Thus, in the IoT network, miners need to be selected appropriately to ensure adequate processing capability. To improve the block verification process, we introduce a method for selecting the best miner which incorporates a learning-to-rank machine learning method. We also introduce a hybrid consensus strategy for aiding decision-making processing. The following sections discuss the miner selection method and the hybrid consensus technique.

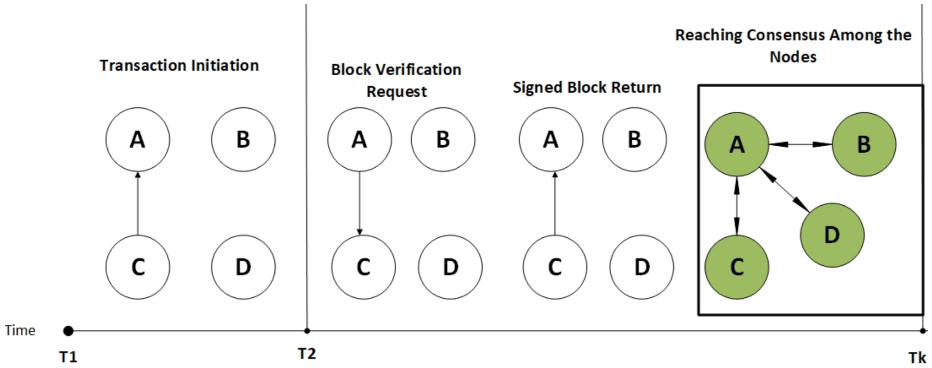
Transaction Initiation
Block Verification Request
Signed Block Return
Reaching Consensus Among the Nodes
A
B
C
D
Time
T1
T2
Tk

Fig. 3. Illustration of the data transfer process using blockchain technology. A sending node C initiates a data transfer request at the time $T1$. At the time $T2$, a selected miner, A examines the transfer credentials, creates a contract and then requests the sending node to sign and return the contract. The miner then broadcasts the signed contract to other miners in the network. At the time Tk, all the miners have reached a consensus to accept the signed contract. A block is created for the signed contract and added to the blockchain.

.

2.1 Machine learning based miner selection

Miner selection is the process of choosing the best node from a set of nodes in a network, used to generate a legitimate block in the blockchain technology. This process is time-consuming especially for IoT networks with many nodes. To simplify the selection process, we introduce a node ranking procedure using the learning-to-rank (LTR) technique [11]. The LTR method has been used previously in product rating [12]. The algorithm takes as inputs the node's properties such as computing power, hash generation rate and block propagation delay, and then finds the optimal sorting of the entire nodes. The node with the most desirable properties is ranked top and can be selected as a miner. The LTR is used to learn a scoring function by mapping the attributes of the nodes to real-valued scores from previously labelled node data. The scoring function is used to sort and rank the nodes as follows:

Let $\tau = \{(\boldsymbol{x}_1, y_1), \ldots, (\boldsymbol{x}_n, y_n)\}$, be a set of data describing n nodes in a decentralised IoT network, where $\boldsymbol{x}_i$ is the i^{th} node and y_i is the corresponding real-valued score associated with the $\boldsymbol{x}_i$ used to rank the node in the past. Each $\boldsymbol{x}_i \in \Re^d$ is represented by a set of attributes (feature vector) of dimension d. $\boldsymbol{x}_i = [\dot{x}_1, \dot{x}_2, \ldots, \dot{x}_d]$, where $\dot{x}_i$ is the i^{th} attribute of the node, such as computing power. The goal is to exploit τ to create a scoring function $f(\cdot)$, such that for any given new node $\boldsymbol{x}_j$, it will generate a score $f(\boldsymbol{x}_j)$. The scoring function can be created using publicly available tools such as ListNet [2] and DeepRank [13]. Thus, for any given j^{th} IoT network with n nodes, we can obtain a sorted list

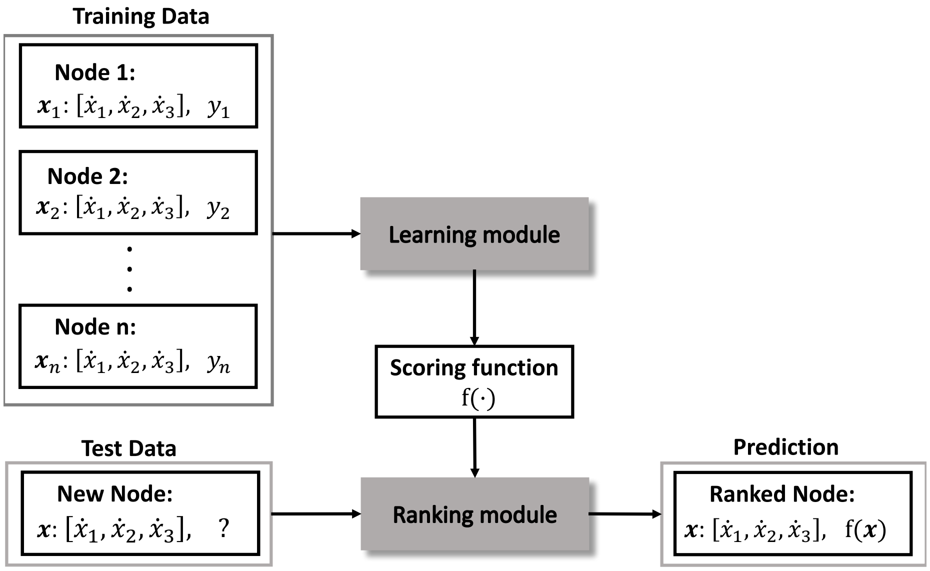
Training Data
Node 1:
$\boldsymbol{x}_1$: $[\dot{x}_1, \dot{x}_2, \dot{x}_3]$, y_1
Node 2:
$\boldsymbol{x}_2$: $[\dot{x}_1, \dot{x}_2, \dot{x}_3]$, y_2
Node n:
$\boldsymbol{x}_n$: $[\dot{x}_1, \dot{x}_2, \dot{x}_3]$, y_n
Learning module
Scoring function
f(·)
Test Data
New Node:
$\boldsymbol{x}$: $[\dot{x}_1, \dot{x}_2, \dot{x}_3]$, ?
Ranking module
Prediction
Ranked Node:
$\boldsymbol{x}$: $[\dot{x}_1, \dot{x}_2, \dot{x}_3]$, f($\boldsymbol{x}$)

Fig. 4. A simple illustration of the LTR ranking procedure. The scoring function can be learned using ListNet [2] or DeepRank [13]. The ranking module is simple sort algorithm.

of scores $s^j = [f(\boldsymbol{x}_1^j), \ldots f(\boldsymbol{x}_n^j)]$ corresponding to the rank of the nodes. Figure 4 illustrates the setup for the learning-to-rank procedure. The creation of the scoring function can be conducted offline and then deploy online for evaluating and ranking the nodes.

2.2 Hybrid consensus algorithm

In blockchain technology, a consensus algorithm must fulfill the following objectives: gathering all the miners agreement, collaboration, participation, and maintaining equal rights to participating miners. In addition to the aforementioned objectives, it is important to be able to detect faulty miners for IoT networks. For this reason, we introduce a hybrid consensus algorithm consisting of binary and average consensus mechanisms [10]. In binary consensus, every miner in the network can hold two status, zero and one. One being functional and zero being faulty. Before two miners communicate and run the set of rules, they compare their current state and assume a new state if their observation is different [1]. In this way, a rogue miner can be detected easily and removed. With average consensus, two miners can reach an agreement by averaging the values of their initial states [15]. While the binary consensus mechanism help with the detection of faulty miners, the average consensus mechanism helps to converge the decision of the miners faster. Algorithm 1 illustrates the hybrid consensus algorithm in a decentralised IoT. The algorithm commences with the

Algorithm 1 Hybrid consensus algorithm for decentralised IoT

```
procedure To reach consensus
    Initiate participating miners
    Initiate average and binary consensus mechanism
    Set consensus criteria (e.g Convergence rate)
    loop:
    Create a new signed contract
    if convergence rate $<$ threshold then
        Invoke the average consensus mechanism
        Broadcast to all participating miners
    if a faulty miner is suspected then
        Invoke the binary consensus mechanism
        Broadcast to all participating miners
    Check if consensus is reached:
    Create a new block for the contract
    Update all the miners' record with the new block information
    Go to loop.
```

creation of a new contract. The participating miners proceed with the consensus process by checking the convergence rate and the possibility of a faulty miner. If the convergence rate is smaller than a predefined threshold, then the average consensus mechanism is activated. However, if there exist some faulty miners, which may disrupt the process of reaching consensus, then the binary consensus mechanism is activated to detect and remove the affected miners.

3 Discussion

In a decentralised IoT, where there is no central control, it is difficult to provide security. Also, the limitations of different communication standards make the working condition of the decentralised IoT challenging. For example, GSM is power-hungry and expensive and Bluetooth technology has a very limited range. Thus, blockchain technology which offers practical solutions to some of the aforementioned limitations is considered appropriate for implementing decentralised IoT. In this paper, we present a framework for secured communication in a decentralised IoT using consortium blockchain, which incorporates machine learning-based miner selection techniques and hybrid consensus mechanism. Our study helps to provides some pointers to future research directions for implementing blockchain technology for IoT. In the following sections, we discuss the research directions.

3.1 Blockchain Mechanism

Blockchain mechanisms including public, private and consortium pose challenges for many IoT applications. A public blockchain incorporates openness, but it is limited in security and poor data transfer time. Private blockchain provides distribution but requires authorisation from some private nodes. Though data transfer time is reduced in a private blockchain, there is no transparency and openness. Consortium blockchain, on the other hand, overcomes the limitations of both public and private blockchain.

3.2 Cryptographic Algorithm

For secured data transfer, encryption is an important issue to consider during nodes communication. Generally, blockchain uses hash functions for encrypting data which is computationally complex. However, for IoT, the cryptographic mechanism should be computationally less complex. An investigation into the various cryptography algorithms is necessary to ensure a computationally efficient encryption algorithm for IoT applications.

3.3 Miner Selection

The selection of miners with good processing capability, hash generation rate and suitable block propagation delay is quite a challenge for many blockchain applications. Because of the roles the miners play in reaching consensus and creating blocks for the blockchain, it is important to adaptively select only those with the best characteristics for the mining task. Machine learning can be used to provide an intelligent way to select a miner. However, with the different machine learning techniques available, choosing a suitable method for a given blockchain-based IoT application can be difficult.

3.4 Consensus Algorithm

A consensus algorithm is helpful for nodes to decide any particular data communication. In a decentralised IoT, since there is no central control, this is even more pertinent. Various consensus algorithms exist for distributed node settings. However, there are limitations when it comes to their adaptation to blockchain-based IoT. The future research direction is to investigate and to get the empirical evaluation for using different consensus algorithms in various settings of blockchain-based IoT.

4 Conclusion

There will be billions of devices soon connected using various communication standards for different IoT applications. For scalability, robustness and proper distributed access to information, the decentralised IoT is the way to go. However, the lack of a central entity makes the security aspect of the decentralised IoT more challenging. Blockchain is a promising technology that can be used to improve security in IoT. In this paper, we present a framework for secured communication in a decentralised IoT network. We discuss the overall blockchain mechanism including the consensus strategy used, the cryptographic algorithm for security and the miner selection method. We also highlight some research directions for the implementation of blockchain technology for other IoT applications. The proposed framework is a work in progress, future work will involve experimentation that will evaluate the performance of the various components of the framework.

References

1. Al-Nakhala, N., Riley, R., Elfouly, T.M.: Binary consensus in sensor motes. In: Proc. of the International Wireless Communications and Mobile Computing Conference. pp. 1337–1342 (2013)
2. Cao, Z., Qin, T., Liu, T.Y., Tsai, M.F., Li, H.: Learning to rank: From pairwise approach to listwise approach. In: Proc. of the International Conference on Machine Learning. pp. 129–136 (2007)
3. Cong, L., He, Z.: Blockchain disruption and smart contracts. The Review of Financial Studies **32**(5), 1754–1797 (2019)
4. Dib, O., Brousmiche, K.L., Durand, A., Thea, E., Hamida, E.: Consortium blockchains: Overview, applications and challenges. International Journal on Advances in Telecommunications **11**(1), 51–64 (2018)
5. Dorri, A., Kanhere, S.S., Jurdak, R., Gauravaram, P.: Blockchain for iot security and privacy: The case study of a smart home. In: proc. of the international conference on pervasive computing and communications workshops. pp. 618–623 (2017)
6. Elisa, N., Yang, L., Chao, F., Cao, Y.: A framework of blockchain-based secure and privacy-preserving e-government system. Wireless Networks pp. 1–11 (2018)
7. Fanning, K., Centers, D.: Blockchain and its coming impact on financial services. Journal of Corporate Accounting Finance **27**(5), 53–57 (2016)
8. Fisher, J., Sanchez, M.: Authentication and verification of digital data utilizing blockchain technology. U.S. Patent Application 15/083,238 (2016)
9. Fortino, G., Guerrieri, A., Russo, W., Savaglio, C.: Integration of agent-based and cloud computing for the smart objects-oriented iot. In: Proc. of the international conference on computer supported cooperative work in design. pp. 493–498 (2014)
10. Kraft, D.: Difficulty control for blockchain-based consensus systems. Peer-to-Peer Networking and Applications **9**(2), 397–413 (2016)
11. Li, H.: A short introduction to learning to rank. Transactions on Information and Systems **94-D**(10), 1854–1862 (2011)
12. Liu, T.Y.: Applications of Learning to Rank, pp. 181–191. Springer Berlin Heidelberg, Berlin, Heidelberg (2011)
13. Pang, L., Lan, Y., Guo, J., Xu, J., Xu, J., Cheng, X.: Deeprank: A new deep architecture for relevance ranking in information retrieval. In: Proc. of the ACM Conference on Information and Knowledge Management. pp. 257–266 (2017)
14. Perera, C., Zaslavsky, A., Christen, P., Georgakopoulos, D.: Sensing as a service model for smart cities supported by internet of things. Transactions on Emerging Telecommunications Technologies **25**(1), 81 – 93 (2014)
15. Xiao, L., Boyd, S., Kim, S.J.: Distributed average consensus with least-mean-square deviation. Journal of parallel and distributed computing **67**(1), 33–46 (2007)
16. Zhang, A., Lin, X.: Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. Journal of medical systems **42**(8), 140– (2018)